

Appl. No. 09/619,633  
Amdt. Dated: September 27, 2004  
Reply to Office Action of: 03/25/2003

### Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

#### Listing of Claims:

1. (currently amended) A method for generating a shared secret value between entities (A, B) in a data communication system, one or more of said entities having a plurality of members (A<sub>i</sub>, B<sub>i</sub>) for participation in said communication system, each member having a long term private key and a corresponding long term public key said method comprising the steps of:
  - (a) generating an ~~entity long term private key and corresponding~~ entity long term public key for each entity by combining the long term ~~private and~~ public keys of each members of the entity.
  - (b) generating a short term private and a corresponding short term public key for each of the members;
  - (c) ~~exchanging making~~ said short term public keys of the available to members within an entity;
  - (d) for each member:
    - i. computing an intra-entity shared key by mathematically combining said short term public keys of each said member;
    - ii. computing an intra-entity public key by mathematically combining its short-term private key, the long term private key and said intra-entity shared key;
  - (e) for each entity combining intra-entity public keys to derive a group short-term public key;
  - (f) each entity ~~transmitting making~~ its intra-entity shared key and its ~~group short-term public key~~ entity long term public key available to said other entities; and
  - (g) each entity computing a common shared key K by combining its group short term public key, with the intra-entity shared key, and an entity long term public key received from the other entity.

Appl. No. 09/619,633

Amdt. Dated: September 27, 2004

Reply to Office Action of: 03/25/2003

2. (original) A method as defined in claim 1, said long term public key being derived from a generator point  $P$  and respective ones of said long term private keys.
3. (original) A method as defined in claim 2, said step (a) including each member selecting a random integer  $x_i$  and multiplying said point  $P$  by  $a$  to obtain  $x_iP$ , the short term public key.
4. (original) A method as defined in claim 3, said intra-entity-shared key being computed by summing said short term public keys.
5. (original) A method as defined in claim 4, said intra-entity public key  $s_i$  being derived by computing  $s_i = x_i + a_i f(\sum x_iP)$ , where  $f$  is a hash function.
6. (original) A method as defined in claim 5, said group short term public key being derived by computing  $\sum s_i$ .
7. (original) A method as defined in claim 1, said long term public keys being derived from a generator  $g$  and respective ones of said long term private keys.
8. (original) A method as defined in claim 7, said step (a) including the step of each member selecting a random integer ( $x_{ij}$ ) and exponentiating a function  $h(g)$  including said generator to a power  $g(x_{ij})$  to obtain the short term public key  $X_{ij} = h(g)^{g(x_{ij})}$ .
9. (original) A method as defined in claim 8, said intra-entity shared key ( $X_i$ ) being computed by each entity multiplying each or its short-term public keys  $X_{ij}$  together.
10. (original) A method as defined in claim 1, including the step of exchanging the entity long term public key between entities.

Appl. No. 09/619,633  
Amdt. Dated: September 27, 2004  
Reply to Office Action of: 03/25/2003

11. (original) A method as defined in claim 10, each entity computing a common shared key  $K$  by combining its group short term public key ( $S_i$ ), with the intra-entity shared key ( $\bar{X}_i$ ), and an entity long term public key received from the other entity.